Notice of Allowability	Application No.	Applicant(s)	
	09/748,441	DAUM ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the examiner's amendment authorized on 1/17/07*.

2. ☒ The allowed claim(s) is/are *16,18,20-22,24,25 and 27-30*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Eric Krischke on 01/17/07.

The claims have been amended as follows:

16. (currently amended) In an appliance communication network, a method for authenticating appliance messages, the method comprising:

maintaining at an appliance communication center a first shared message counter that counts messages communicated between the appliance communication center and a first appliance, the first shared message counter shared between the communication center and the first appliance;

maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and a second appliance, the second shared message counter provides a count separate from a count provided by the first shared message counter;

generating a first authentication word by applying an appliance message, a shared authentication keying variable K shared between the appliance communication center and the first appliance, and the first shared message counter, as stored in the communication center, to an authentication algorithm;

transmitting the appliance message and the first authentication word as an authenticated message to the first appliance;

receiving the authenticated message at the first appliance;

applying a third shared message counter, the shared authentication keying variable, as stored in the first appliance, and the appliance message to the authentication algorithm to generate the second authentication word;

comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message;

installing a master keying variable within the first appliance and the appliance communication center; and

changing, within the first appliance, the shared authentication keying variable by applying the shared authentication keying variable and the master keying variable to the authentication algorithm to generate a new shared authentication keying variable~~; and~~

~~authenticating the appliance message using the new shared authentication keying variable~~.

17. (canceled)

19. (canceled)

20 (currently amended) The method of claim ~~19~~16, wherein generating a first authentication word by applying comprises:

establishing a working register R, comprising at least bytes R0, R1, R2, R3;

initializing R3 to a directional code, representing a transmission from the appliance communication center to the first appliance;

initializing at least R2, R1, and R0 to a plurality of bytes C2, Cl, and C0 of the first shared message counter, as stored in the communication center, respectively;

iteratively performing at least one arithmetic, logical and shifting operation on R; and

setting the first authentication word equal to the value contained in R.

25. (currently amended) A system comprising:

a plurality of appliances including a first appliance and a second appliance; and

an appliance communication center including:

network connections terminating at the appliances;

a processing circuit;

a memory storing a master keying variable shared between the appliance communication center and the first appliance, an authentication keying variable shared between the appliance communication center and the first appliance, and a plurality of shared counters including a first shared message counter and a second shared message counter, the first shared message counter shared between the appliance communication center and the first appliance, the second shared message counter shared between the communication center and the second appliance, the first shared message counter configured to provide a count separate from a count provided by the second shared message counter, the first and second shared message counters configured to be non-resettable, the memory further storing instructions for:

maintaining at the appliance communication center the first shared message counter;

generating a first authentication word by applying an appliance message, a shared authentication keying variable, and the first shared message counter, as stored in the appliance communication center, to an authentication algorithm;

transmitting the appliance message and the first authentication word as an authenticated message to the first appliance; and

~~transmitting a command to install a master keying variable within the first appliance and the appliance communication center; and~~

transmitting a command to the first appliance to change the shared authentication keying variable by applying the shared authentication keying variable and the master keying variable to the authentication algorithm ~~to generate a new shared authentication keying variable~~.

28. (currently amended) A system comprising:

an appliance communication center;

a first appliance including:

a first shared message counter shared between the first appliance and the appliance communication center;

a shared master keying variable shared between the first appliance and the appliance communication center;

a shared authentication keying variable shared between the first appliance and the appliance communication center;

a processor; and

a memory coupled to the processor, the memory storing instructions for execution by the processor for:

receiving an authenticated message, including a first authentication word and an appliance message, at the first appliance;

generating a second authentication word by applying the first shared message counter, ~~as stored in the first appliance, a~~ the shared authentication keying variable, and the appliance message to an authentication algorithm; and

comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message; and

a second appliance separate from the first appliance~~; and~~

~~an~~wherein the appliance communication center including a second shared message counter and a third shared message counter, the second shared message counter shared between the appliance communication center and the first appliance, the third shared message counter shared between the communication center and the second appliance, and the third shared message counter configured to provide a count separate from a count provided by the second shared message counter[[,]];

wherein the memory ~~configured to~~further stores instructions ~~install a master keying variable within the first appliance and the appliance communication center, and~~ for generating a new shared authentication keying variable, upon the first appliance receiving a command from the appliance communication center, by applying the shared authentication keying variable and the shared master keying variable to the authentication algorithm ~~to generate a new shared authentication keying variable~~.

30. (currently amended) In an appliance communication network, a method for authenticating appliance messages, the method comprising:

maintaining at a first appliance a first non-resettable shared message counter, the first non-resettable shared message counter shared between the first appliance and a remotely located appliance communication center;

maintaining at the appliance communication center a second non-resettable shared message counter that counts messages communicated between the appliance communication center and the first appliance;

maintaining at the appliance communication center a third non-resettable shared message counter that counts messages communicated between the appliance communication center and a second appliance, the third non-resettable shared message counter provides a count separate from a count provided by the second non-resettable shared message counter;

generating a first authentication word by applying an appliance message, a shared authentication keying variable shared between the first appliance and the appliance communication center, and the first non-resettable shared message counter, as stored in the first appliance, to an authentication algorithm;

transmitting the appliance message and the first authentication word as an authenticated message to the appliance communication center; ~~and~~

receiving the authenticated message at the appliance communication center;

applying the second non-resettable shared message counter, the shared authentication keying variable, as stored in the appliance communication center, and the appliance message to the authentication algorithm to generate a second authentication word;

comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message;

installing a master keying variable within the first appliance and the appliance communication center; and

changing, within the first appliance, the shared authentication keying variable by applying the shared authentication keying variable and the master keying variable to the authentication algorithm to generate a new shared authentication keying variable; ~~and~~

~~authenticating the appliance message using the new shared authentication keying variable~~.

31. (canceled)

2. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method and system for authenticating messages communicated between a first appliance and an appliance communication center, wherein both entities have a shared authentication keying variable and a shared message counter that counts messages communicated between them; wherein the appliance communication center maintains another shared message counter for communication with another appliance; wherein a transmitting entity applies the appliance message to be transmitted, the shared authentication keying variable, and the shared message counter to an authentication algorithm to generate an authentication word which will be transmitted with the appliance message; wherein a receiving entity applies the received appliance message, the shared authentication keying variable, and the shared message counter to the authentication algorithm to generate an authentication word, and compares the generated authentication word with the received authentication word to determine the authenticity of the appliance message. More specifically, independent claims 16, 25, 28 and 30 identify the uniquely distinct features: changing, within the first appliance, the shared authentication keying variable by applying the shared authentication keying variable, and a master keying variable shared between the appliance and the appliance communication center to the authentication algorithm to generate

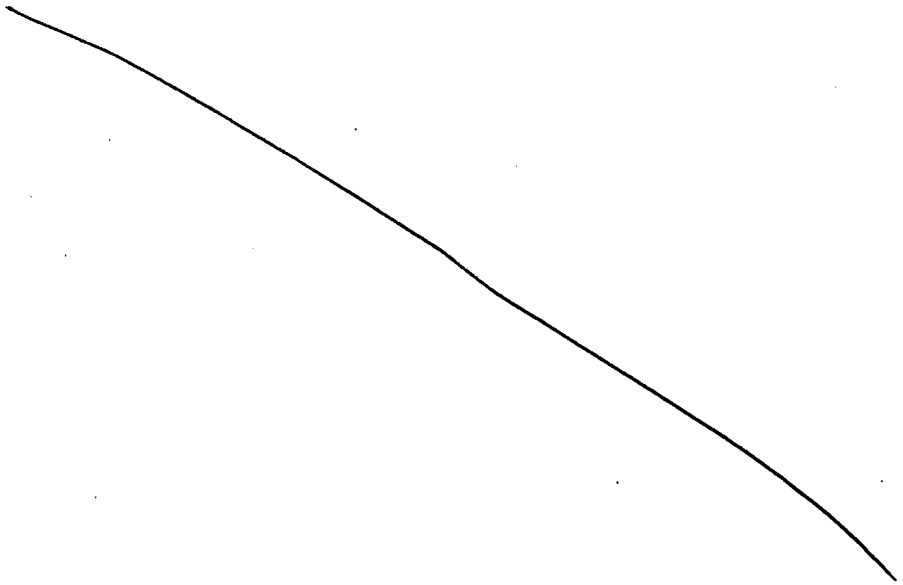
a new shared authentication keying variable. The closest prior art include: (i) Sharrow (6,061,668) teaches authenticating messages communicated between an appliance and an appliance communication center using a checksum value (fig. 2 and corresponding text); (ii) Hoffman et al (6,366,682) teaches maintaining multiple shared message counters by an entity when the entity communicates with two or more other entities; each of the shared message counters is separately maintained for each of the other entities (fig. 8; col. 29, line 42 – col. 30, line 59); (iii) Elgamal et al (5,825,890) teaches generating an authentication word for a message to be transmitted using the message, the value of a shared message counter and a shared keying variable shared between the transmitting and receiving entities (col. 17, line 56 – col. 18, line 17; col. 18, lines 26-30); Elgamal also teaches generating a new shared keying variable applying a master keying variable and another data value to a hash function (col. 7, lines 41-59); and (iv) Srivastava et al. (7,103,185) teaches generating a new key by applying the current key to a hash function (col. 16, lines 51-65). However, Sharrow, Elgamal, Hoffman, and Srivastava, either alone or in combination, do not teach the specific features mentioned above. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claims are

therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

MD
1/18/07

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100